Investigadores de seguridad cibernética descubrieron una campaña de malware en curso que depende en gran medida del lenguaje de scripting AutoHotkey (AHK) para entregar múltiples troyanos de acceso remoto (RAT) como Revenge RAT, LimeRAT, AsyncRAT, Houdini y Vjw0rm en sistemas Windows de destino.

Se han detectado al menos 4 versiones distintas de la campaña a partir de febrero de 2021, según los investigadores de Morphisec Labs.

> *«La campaña de entrega de RAT comienza con un script compilado de AutoHotKey (AHK). Este es un ejecutable independiente que contiene lo siguiente: el intérprete AHK, el script AHK y cualquier archivo que haya incorporado mediante el comando FileInstall. En esta campaña, los atacantes incorporan scripts/ejecutables maliciosos junto con una aplicación legítima para disfrazar sus intenciones»,* dijeron los investigadores.

AutoHotKey es un lenguaje de scripting personalizado de código abierto para Microsoft Windows que está destinado a proporcionar teclas de acceso rápido fáciles para la creación de macros y la automatización de software, lo que permite a los usuarios automatizar tareas repetitivas en cualquier aplicación de Windows.

Independientemente de la cadena de ataque, la infección comienza con un ejecutable AHK que procede a soltar y ejecutar distintos VBScripts que eventualmente cargan el RAT en la máquina comprometida. En una variante del ataque detectado por primera vez el 31 de marzo, el adversario detrás de la campaña encapsuló la RAT eliminada con un ejecutable AHK, además de deshabilitar Microsoft Defender mediante la implementación de un script por lotes y un archivo de acceso directo que apunta a dicho script.

Se descubrió que una segunda versión del malware bloquea las conexiones a soluciones antivirus populares al alterar el archivo de hosts de la víctima. *«Esta manipulación niega la resolución de DNS para esos dominios al resolver la dirección IP del host local en lugar de la real»*, agregaron los investigadores.

Por otro lado, una cadena de carga observada el 26 de abril, implicó la entrega de LimeRAT a través de un VBScript ofuscado, que luego se decodifica en un comando de PowerShell que recupera una carga útil de C# que contiene el ejecutable de la etapa final de un servicio de plataforma de intercambio similar a Pastebin llamado *«stikked.ch»*.

Finalmente, una cuarta cadena de ataque descubierta el 21 de abril, utilizó un script AHK para ejecutar una aplicación legítima, antes de soltar un VBScript que ejecuta un script PowerShell en memoria para buscar el cargador de malware HCrypt e instalar AsyncRAT.

Los investigadores de Morphisec atribuyeron todas las diferentes cadenas de ataque al mismo actor de amenaza, citando similitudes en el script AHK y superposiciones en las técnicas utilizadas para deshabilitar Microsoft Defender.

> *«A medida que los actores de amenazas estudian los controles de seguridad básicos como emuladores, antivirus y UAC, desarrollan técnicas para eludirlos y evadirlos. Los cambios de técnica detallados en este informe no afectaron el impacto de estas campañas. Los objetivos tácticos siguieron siendo los mismos. Mas bien, los cambios de técnica fueron eludir los controles de seguridad pasivos. Un denominador común entre estas técnicas evasivas es el abuso de la memoria del proceso porque es típicamente un objetivo estático y predecible para el adversario»,* dijeron los investigadores.

Esta no es la primera vez que los atacantes abusan de AutoHotKey para eliminar malware. En diciembre de 2020, los investigadores de Trend Micro descubrieron un ladrón de credenciales escrito en el lenguaje de programación de AutoHotKey que destacaba a las instituciones financieras de Estados Unidos y Canadá.